AI-Powered Infrastructure Threat Detection for SMBs

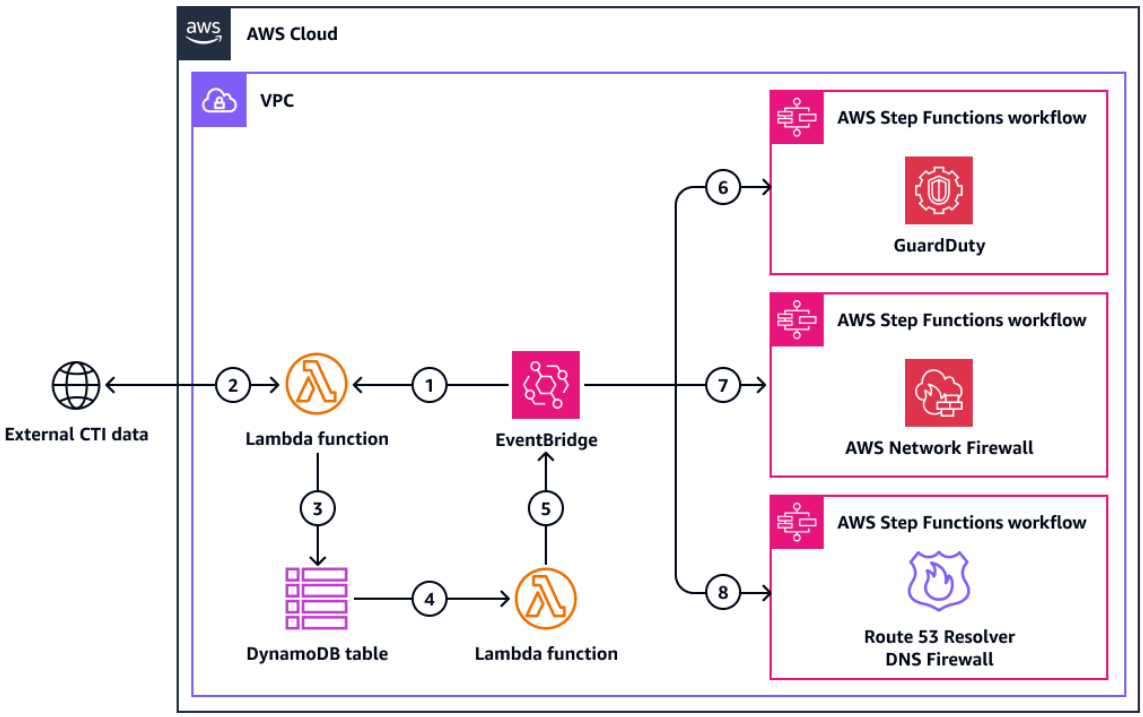
Automated, ML-driven security monitoring and response for small teams with no dedicated cybersecurity staff

The Business Problem

Most SMBs lack the budget for a dedicated security operations team, yet face the same threats as large enterprises. According to the 2024 Verizon Data Breach Investigations Report, 46% of all cyber breaches impact businesses with fewer than 1,000 employees. Without continuous monitoring, a compromised server or stolen credential can go undetected for weeks, leading to data loss, regulatory fines, and eroded customer trust. Manual log review does not scale, and traditional Security Information and Event Management (SIEM) tools require specialized staff to deploy and tune. The result: small IT teams spend hours reacting to incidents they should have caught automatically.

Recommended Solution

Deploy Amazon GuardDuty for continuous, ML-powered threat detection and AWS Security Hub for centralized compliance monitoring, connected by an automated response pipeline that remediates common issues without human intervention.



Architecture: End-to-end threat detection and automated response pipeline, from GuardDuty finding generation through Security Hub aggregation, EventBridge routing, and serverless remediation with team notification.

GuardDuty analyzes account activity, network traffic, and DNS queries to surface threats like credential misuse and unauthorized access. Security Hub consolidates those findings alongside compliance checks into a single console with a 0-to-100 security score. The open-source Automated Security Response on AWS (ASR) solution adds pre-built remediation playbooks deployed separately via AWS CloudFormation, so a one-to-three person IT team gets enterprise-grade protection with no servers to manage. Both services are pay-as-you-go with 30-day free trials, delivering immediate time-to-value.

Technical Architecture

The solution follows a detect, aggregate, route, remediate, and notify pipeline built entirely on managed and serverless services.

- **Threat detection:** Amazon GuardDuty continuously analyzes AWS CloudTrail management events, Amazon Virtual Private Cloud (VPC) Flow Logs, and DNS query logs using ML and anomaly detection. No agents or log pipelines are required for foundational monitoring.
- **Aggregation and compliance:** AWS Security Hub collects GuardDuty findings alongside automated compliance checks (CIS Benchmarks, AWS Foundational Security Best Practices, NIST, PCI DSS) into a unified dashboard with a consolidated security score.
- **Automated response:** Amazon EventBridge captures findings in near real time and routes them to AWS Step Functions, which orchestrates remediation through AWS Lambda and AWS Systems Manager Automation documents. ASR provides pre-packaged playbooks covering dozens of common misconfigurations.
- **Notification:** Amazon Simple Notification Service (SNS) delivers alerts via email or chat, closing the loop on every finding.
- **Networking and security:** Network isolation, least-privilege access, and encryption are enforced through native AWS controls, keeping operational burden low.
- **Monitoring:** Centralized logging and operational metrics provide audit trails and pipeline health visibility without a separate monitoring stack.

Key Considerations

Decision	Guidance
Enable all GuardDuty protection plans or start with foundational detection?	Start with foundational detection (CloudTrail, VPC Flow Logs, DNS). Add Runtime Monitoring after validating findings during the 30-day free trial.
Deploy ASR playbooks for all compliance standards or select one?	Begin with AWS Foundational Security Best Practices. Add CIS or PCI DSS playbooks only if your business has specific regulatory requirements.
Automate remediation immediately or start with alerts only?	Start notification-only so your team can review findings. Enable auto-remediation for low-risk actions (like re-enabling logging) within 30 days, then expand.
Single-account or multi-account setup?	Fewer than three accounts: single-account deployment is sufficient. For growing organizations, use AWS Organizations with a delegated Security Hub administrator.

Expected Outcomes

- **Threat detection in minutes, not weeks:** GuardDuty begins generating findings immediately upon enablement with zero configuration (Getting started with GuardDuty).
- **90% reduction in manual security review time:** Automated compliance checks and consolidated findings replace manual log review and spreadsheet tracking (AWS Security Hub features).
- **Deployment in 1 to 5 days:** A partner-led engagement can deliver the full detection-and-response pipeline within a business week (ASR deployment guide).
- **Continuous compliance visibility:** Automated checks against industry standards provide audit-ready posture reporting without dedicated compliance staff.
- **Predictable, consumption-based costs:** Pay-as-you-go pricing with free tiers on orchestration components means costs scale with your environment, not with a fixed license fee (GuardDuty pricing, Security Hub pricing).